### IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| Application No: | 10/578,638 |
| Applicant: | Hiroki Kaihori |
| Filed: | May 9, 2006 |
| Title: | VEHICLE ANTITHEFT SYSTEM |
| TC/A.U.: | 2437 |
| Examiner: | Jeffery L. Williams |
| Confirmation No.: | 3451 |
| Notice of Appeal Filed: | June 2, 2010 |
| Docket No.: | MAT-8849US |

### APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA  22313-1450

S I R :

Responsive to the Notice of Panel Decision dated July 12, 2010, Appellant is submitting this Appeal Brief for the above-identified application.

This Brief is presented in the format required by 37 C.F.R. § 41.37, in order to facilitate review by the Board.  In compliance with 37 C.F.R. § 41.37(a)(1), this Brief is being filed within the time allowed for response to the action from which the Appeal was taken or within two months from the date of the Notice of Appeal, whichever is later.

The fees for filing a Brief in support of an Appeal under 37 C.F.R. § 41.20(b)(2), together with any extension fee required in connection with the filing of this Brief, are provided herewith.

#### I.      REAL PARTY IN INTEREST

The real Party In Interest in this matter is the Assignee, Panasonic Corporation.

#### II.     RELATED APPEALS AND INTERFERENCES

## II.    RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences which will directly affect or be directly affected by, or have a bearing on the Board's decision in the pending Appeal.

## III.    STATUS OF CLAIMS

Claims 1-24 are pending and stand rejected.   Claims 1-24 are appealed.

## IV.    STATUS OF AMENDMENTS

The present application is under Final Rejection.   All of the previous amendments have been entered.

## V.    SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to vehicle anti-theft systems.   Provided next is a summary of the subject matter for each of independent claims 1-4.

### Independent Claim 1

As illustrated by Appellant's Fig. 1, Appellant's vehicle anti-theft system includes immobilizer unit 8 and portable unit 15.  The immobilizer unit 8 includes first data processor means 2, a first communication part 3 connected with the first data processor means 2, a first antenna 4 connected with the first communication part 3, a first storage 5 connected with the first data processor means 2 and a second storage 6 connected with the first data processor means 2. The first storage 5 preliminarily stores first data for mutual authentication.  (Page 5, line 14-page 6, line 1 of the Substitute Specification filed on May 9, 2006.)  The first data processor means 2 can include a CPU.  (Page 6, lines 27-28.)

The portable unit 15 includes second data processor means 9, a second communication part 10 connected with the second data processor means 9, a second antenna 11 connected with the second communication part 10, a third storage 12 connected with the second data processor means 9 and a fourth storage

13 connected with the second data processor means. (Page 6, lines 2-8.) The third storage 12 preliminarily stores the first data for mutual authentication. (Page 6, lines 6-8.) The fourth storage 13 preliminarily stores second data for mutual authentication different from the first data for mutual authentication. (Page 8, lines 12-14.) The second data processor means 9 can include a CPU. (Page 6, line 9.)

The immobilizer unit 8 further includes an information reception part 1 connected with the first data processor means 2. (Page 5, lines 21-22.) As shown in Fig. 2, when a first instruction is fed into the information reception part 1 (page 6, lines 15-19; and S1 in Fig. 2), the first data processor means 2 and the second data processor means 9 authenticate each other by a first authentication (page 6, line 26-page 7, line 1; and S4 in Fig. 2). As shown in Fig. 3, the first authentication comprises: (1) the first data processor means 2 transmitting via the first antenna 4 an encrypted data based on the first data for mutual authentication stored in the first storage 5 (page 7, lines 3-13; and S43 in Fig. 3) and (2) the second data processor means 9 receiving the encrypted data via the second antenna 11 (page 7, lines 14-16), decrypting the encrypted data (page 7, lines 14-16; and S44 in Fig. 3) and comparing the decrypted data to the first data for mutual authentication stored in the third storage 12 (page 7, lines 16-21; and S45 in Fig. 3).

As shown in Fig. 2, the first data processor means 2 and the second data processor means authenticate each other by a second authentication (page 8, lines 9-14; and S6-S10 in Fig. 2), responsive to the first authentication between the first data processor means and the second data processor means (page 6, line 27-page 7, line 2; page 8, lines 9-14; and S5 in Fig. 2). The second authentication comprises: 1) the second data processor means 9 transmitting the second data for mutual authentication stored in the fourth storage 13 via the second antenna 11 (page 8, lines 13-17; and S7 in Fig. 2), 2) the first data processor means 2 further storing, into the second storage 6, the second data for mutual authentication received via the first antenna 4 (page 8, lines 17-19; and S8 in Fig. 2) and transmitting the second data for mutual authentication stored in the second storage 6 via the first antenna 4 (page 8, lines 19-22; and S9 in Fig. 2), and 3) the second data processor means 9 further storing, into the third storage 12, the second data for mutual authentication received via the second antenna 11 (page 8, lines 22-25; and S10 in Fig. 2).

Independent Claim 2

As illustrated by Appellant's Fig. 9, Appellant's vehicle anti-theft system includes immobilizer unit 8 and portable unit 15. The immobilizer unit 8 includes first data processor means 2, a first communication part 3 connected with the first data processor means 2, a first antenna 4 connected with the first communication part 3, a first storage 5 connected with the first data processor means 2 and a second storage 6 connected with the first data processor means 2. The first storage 5 preliminarily stores first data for mutual authentication. (Page 5, line 14-page 6, line 1). The second storage 6 preliminarily stores second data for mutual authentication different from the first data for mutual authentication. (Page 12, lines 21-27; and page 13, lines 6-9.) The first data processor means 2 can include a CPU. (Page 6, lines 27-28.)

The portable unit 15 includes second data processor means 9, a second communication part 10 connected with the second data processor means 9, a second antenna 11 connected with the second communication part 10 and a third storage 12 connected with the second data processor means 9. (Page 6, lines 2-8.) The third storage 12 preliminarily stores the first data for mutual authentication. (Page 6, lines 6-8.) The second data processor means 9 can include a CPU. (Page 6, line 9.)

The immobilizer unit 8 further includes an information reception part 1 connected with the first data processor means 2. (Page 5, lines 21-22.) As shown in Fig. 10, when a first instruction is fed into the information reception part 1 (page 6, lines 15-19; and S1 in Fig. 10), the first data processor means 2 and the second data processor means 9 authenticate each other by a first authentication (page 6, line 26-page 7, line 1; and S4 in Fig. 10). As shown in Fig. 3, the first authentication comprises: (1) the first data processor means 2 transmitting via the first antenna 4 an encrypted data based on the first data for mutual authentication stored in the first storage 5 (page 7, lines 3-13; and S43 in Fig. 3) and (2) the second data processor means 9 receiving the encrypted data via the second antenna 11 (page 7, lines 14-16), decrypting the encrypted data (page 7, lines 14-16; and S44 in Fig. 3) and comparing the decrypted data to the first data for mutual authentication stored in the third storage 12 (page 7, lines 16-21; and S45 in Fig. 3).

As shown in Fig. 10, the first data processor means 2 and the second data processor means 9 authenticate each other by a second authentication (page 12, line 28-page 13, line 5; and S5-S97 in Fig. 10), responsive to the first authentication between the first data processor means 2 and the second data processor means 9 (page 6, line 27-page 7, line 2; page 12, line 28-page 13, line 3 and S5 in Fig. 10). The second authentication comprises: 1) the first data processor means 2 transmitting the second data for mutual authentication that is stored in the second storage 6 via the first antenna 4 (page 12, line 28-page 13, line 3; and S96 in Fig. 10) and 2) the second data processor means 2 storing, into the third storage 12, the second data for mutual authentication received via the second antenna 11 (page 13, lines 3-5; and S97 in Fig. 10).

## Independent Claim 3

As illustrated by Appellant's Fig. 9, Appellant's vehicle anti-theft system includes immobilizer unit 8 and portable unit 15. The immobilizer unit 8 includes first data processor means 2, a first communication part 3 connected with the first data processor means 2, a first antenna 4 connected with the first communication part 3, a first storage 5 connected with the first data processor means 2 and a second storage 6 connected with the first data processor means 2. The first storage 5 preliminarily stores first data for mutual authentication. (Page 5, line 14-page 6, line 1). The first data processor means 2 can include a CPU. (Page 6, lines 27-28.)

The portable unit 15 includes second data processor means 9, a second communication part 10 connected with the second data processor means 9, a second antenna 11 connected with the second communication part 10 and a third storage 12 connected with the second data processor means 9. (Page 6, lines 2-8.) The third storage 12 preliminarily stores the first data for mutual authentication. (Page 6, lines 6-8.) The second data processor means 9 can include a CPU. (Page 6, line 9.)

The immobilizer unit 8 further includes an information reception part 1 connected with the first data processor means 2. (Page 5, lines 21-22.) As shown in Fig. 11, when a first instruction is fed into the information reception part 1 (page 6,

lines 15-19; and S1 in Fig. 11), the first data processor means 2 and the second data processor means 9 authenticate each other by a first authentication (page 6, line 26-page 7, line 1; and S4 in Fig. 11). As shown in Fig. 3, the first authentication comprises: (1) the first data processor means 2 transmitting via the first antenna 4 an encrypted data based on the first data for mutual authentication stored in the first storage 5 (page 7, lines 3-13; and S43 in Fig. 3) and (2) the second data processor means 9 receiving the encrypted data via the second antenna 11 (page 7, lines 14-16), decrypting the encrypted data (page 7, lines 14-16; and S44 in Fig. 3) and comparing the decrypted data to the first data for mutual authentication stored in the third storage 12 (page 7, lines 16-21; and S45 in Fig. 3).

As shown in Fig. 11, the first data processor means 2 and the second data processor means 9 authenticate each other by a second authentication (page 13, lines 20-24; and S5-S110 in Fig. 11), responsive to the first authentication between the first data processor means 2 and the second data processor means 9 (page 6, line 27-page 7, line 2; page 13, lines 20-24; and S5 in Fig. 11). The second authentication comprises: 1) the first data processor means 2 requesting the second data processor means 9 via the first antenna 4 to generate second data for mutual authentication different from the first data for mutual authentication (page 13, lines 20-24; and S106 in Fig. 11), 2) responsive to the request from the first data processor means 2, the second data processor means 9 further generating, storing into the third storage 12, and transmitting via the second antenna 11, the second data for mutual authentication (page 13, line 24-page 14, line 4; and S107 in Fig. 11), 3) the first data processor means 2 storing, into the second storage 6, the second data for mutual authentication received via the first antenna 4 (page 14, lines 4-5; and S108 in Fig. 11) and transmitting the second data for mutual authentication stored in the second storage 6 via the first antenna 4 (page 14, lines 5-8; and S109 in Fig. 11) and 4) the second data processor means 9 further storing, into the third storage 12, the second data for mutual authentication received via the second antenna 11 (page 14, lines 8-10; and S110 in Fig. 11).

<div align="center">Independent Claim 4</div>

As illustrated by Appellant's Fig. 9, Appellant's vehicle anti-theft system includes immobilizer unit 8 and portable unit 15. The immobilizer unit 8

includes first data processor means 2, a first communication part 3 connected with the first data processor means 2, a first antenna 4 connected with the first communication part 3, a first storage 5 connected with the first data processor means 2 and a second storage 6 connected with the first data processor means 2. The first storage 5 preliminarily stores first data for mutual authentication. (Page 5, line 14-page 6, line 1). The first data processor means 2 can include a CPU. (Page 6, lines 27-28.)

The portable unit 15 includes second data processor means 9, a second communication part 10 connected with the second data processor means 9, a second antenna 11 connected with the second communication part 10 and a third storage 12 connected with the second data processor means 9. (Page 6, lines 2-8.) The third storage 12 preliminarily stores the first data for mutual authentication. (Page 6, lines 6-8.) The second data processor means 9 can include a CPU. (Page 6, line 9.)

The immobilizer unit 8 further includes an information reception part 1 connected with the first data processor means 2. (Page 5, lines 21-22.) As shown in Fig. 12, when a first instruction is fed into the information reception part 1 (page 6, lines 15-19; and S1 in Fig. 12), the first data processor means 2 and the second data processor means 9 authenticate each other by a first authentication (page 6, line 26-page 7, line 1; and S4 in Fig. 12). As shown in Fig. 3, the first authentication comprises (1) the first data processor means 2 transmitting via the first antenna 4 an encrypted data based on the first data for mutual authentication stored in the first storage 5 (page 7, lines 3-13; and S43 in Fig. 3) and (2) the second data processor means 9 receiving the encrypted data via the second antenna 11 (page 7, lines 14-16), decrypting the encrypted data (page 7, lines 14-16; and S44 in Fig. 3) and comparing the decrypted data to the first data for mutual authentication stored in the third storage 12 (page 7, lines 16-21; and S45 in Fig. 3).

As shown in Fig. 12, the first data processor means 2 and the second data processor means 9 authenticate each other by a second authentication (page 14, lines 21-23; and S5-S119 in Fig. 12), responsive to the first authentication between the first data processor means 2 and the second data processor means 9 (page 6, line 27-page 7, line 2; page 14, lines 21-23; and S5 in Fig. 12). The

second authentication comprises: 1) the first data processor means 2 generating (page 14, lines 21-24; and S116 in Fig. 12), storing into the second storage 6 (page 14, lines 23-24; and S117 in Fig. 12), and transmitting via the first antenna 4, second data for mutual authentication different from the first data for mutual authentication (page 14, lines 24-26; and S118 in Fig. 12) and 2) the second data processor means 9 storing, into the third storage 12, the second data for mutual authentication received via the second antenna 11 (page 14, lines 26-28; and S119 in Fig. 12).

## VI.    GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1)    The specification has been objected to as failing to provide antecedent basis for the claimed subject matter.

2)    Claims 1-24 have been rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

3)    Claims 1-24 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite.

4) Claims 1-24 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Tsuji et al. (2004/0056776) (referred to herein as Tsuji) in view of Hisada (US 6,043,752) (referred to herein as Hisada).

## VII.    ARGUMENT

**A.  Objection to the Specification as failing to Provide Proper Antecedent Basis for the Claimed Subject Matter.**

On pages 2-3 of the Final Office Action dated March 2, 2010, the specification was objected to as allegedly failing to provide proper antecedent basis for the claimed subject matter.  In particular, it was asserted that the specification failed to provide proper antecedent basis for the recitations of "means for authenticating each other by a first authentication" and "means for authenticating each other by a second authentication."  In response to the Office Action, claims 1-4 were amended to remove the phrase "includes means for authenticating."  Appellant notes that, although Appellant's amended claims were entered, the Advisory Action

dated May 18, 2010, does not address whether the objection to the specification was withdrawn. Appellant contends that the amendments filed on May 3, 2010 overcome the objection. Accordingly, Appellant respectfully requests that the objection to the specification be withdrawn.

**B.  Rejection of Claims 1-24 under 35 U.S.C. § 112, First Paragraph, as failing to Comply with the Written Description Requirement.**

On page 3 of the Final Office Action, claims 1-24 were rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.  In particular, it was asserted that "Applicant has not pointed out where the new (or amended) claim is supported, nor does there appear to be a written description of the claim limitations in the application as filed." As discussed above, claims 1-4 were amended to remove the phrase "includes means for authenticating." Appellant notes that the Advisory Action also does not address whether the rejection of claims 1-24 under 35 U.S.C. § 112, first paragraph was withdrawn. Appellant contends that the amendments filed on May 3, 2010 overcome the rejection.  Accordingly, Appellant respectfully requests that the rejection of claims 1-24 under 35 U.S.C. § 112, first paragraph be withdrawn.

**C.  Rejection of Claims 1-24 under 35 U.S.C. § 112, Second Paragraph, as being Indefinite.**

On pages 4-5 of the Final Office Action, claims 1-24 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite.  In particular, it was asserted that the phrase "means for authenticating each other by a first authentication" and "means for authenticating each other by a second authentication" renders the scope of the claims indefinite.  As discussed above, claims 1-4 were amended to remove the phrase "includes means for authenticating." Appellant once again notes that the Advisory Action does not address whether the rejection of claims 1-24 under 35 U.S.C. § 112, second paragraph is withdrawn. Appellant contends that the amendments filed on May 3, 2010 overcome the rejection. Accordingly, Appellant respectfully requests that the rejection of claims 1-24 under 35 U.S.C. § 112, second paragraph, be withdrawn.

On pages 5-6 of the Final Office Action, claims 5, 10, 15 and 20 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. In particular, it was asserted that the phrase "the second accumulation data," recited in "lines 8 and 14 of claim 5" lacks antecedent basis. Claims 10, 15 and 20 were rejected for similar reasons. Claims 5, 10, 15, and 20 (as well as claims 6, 11, 16 and 21) were amended accordingly. Appellant notes that the Advisory Action does not address whether the rejection of claims 5, 10, 15 and 20 under 35 U.S.C. § 112, second paragraph is withdrawn. Appellant contends that the amendments filed on May 3, 2010 overcome the rejection. Accordingly, Appellant respectfully requests that the rejection of claims 5, 10, 15 and 20 under 35 U.S.C. §112, second paragraph be withdrawn.

**D.   Rejection of Claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Tsuji in view of Hisada.**

The aforementioned rejection is respectfully traversed for at least the reasons set forth below.

Appellant's claim 1 relates to a vehicle anti-theft system including an immobilizer unit and a portable unit. Particularly, independent claim 1, recites the following:

> ...an immobilizer unit including ... first data processor means ...

> ...a portable unit including... second data processor means...; and _fourth storage_... _preliminarily storing second data_ for mutual authentication different from the first data for mutual authentication...

> ... the first data processor means and the second data processor means _authenticate each other by a first authentication_ comprising: (1) the first data processor means transmitting ... an encrypted data _based on the first data for mutual authentication_ stored in the first storage and (2) the second data processor means receiving the encrypted data ... decrypting the encrypted data and _comparing the decrypted data to the first data for mutual authentication_ stored in the third storage; and

> ... the first data processor means and the second data processor means _authenticate each other by a second authentication_, _responsive to the first authentication_ between the first data

> processor means and the second data processor means, comprising: 1) the second data processor means <u>transmitting the second data for mutual authentication</u> stored in the fourth storage ... 2) the first data processor means further <u>storing</u>, into the second storage, <u>the second data for mutual authentication</u> ... and <u>transmitting the second data for mutual authentication</u> stored in the second storage ... and 3) the second data processor means further <u>storing</u>, into the third storage, <u>the second data for mutual authentication</u> received... (Emphasis Added)

Appellant's claim 1 includes features which are neither disclosed nor suggested by the cited art. Namely, first and second data processor means, of the respective immobilizer unit and the portable unit, which authenticate each other by the combination of: 1) <u>a first authentication</u> which includes passing and comparing <u>first data</u> between the immobilizer and portable units and 2) <u>a second authentication, responsive to the first authentication</u>, which includes passing <u>second data</u> between the immobilizer and portable units. One issue under appeal is whether or not Tsuji or Hisada disclose or suggest first and second data processor means which authenticate each other by a second authentication using second data, responsive to the first authentication.

On pages 6-7 of the Final Office Action, it is asserted that Tsuji discloses the claimed system, based on Figs. 1 and 11. Page 7 of the Final Office Action also argues that "system or apparatus claims must be *structurally* distinguishable from the prior art." Pages 7-9 of the Final Office Action subsequently asserts that Tsuji teaches "aspects pertaining the operation of the claimed system or apparatus, the examiner notes that the prior art will continue to be referenced largely for the applicant's benefit and understanding of the prior art reference."

On pages 8-9 of the Final Office Action, the Examiner asserts that Tsuji teaches first and second authentication. In particular, paragraphs [0084], [0088] and [0090] of Tsuji were relied upon as teaching first authentication (page 8 of the Final Office Action); and paragraphs [0043-0044], [0049] and [0053] of Tsuji et al. were relied upon as teaching a second authentication (page 9 of the Final Office Action).

Appellant subsequently submitted a response to the Final Office Action, dated May 3, 2010 including additional arguments that Tsuji does not teach first and

second data processor means that authenticate each other using a second authentication, responsive to a first authentication, with second data.

In the Advisory Action dated May 18, 2010, the Advisory Action did not address Appellant's remarks dated May 3, 2010. Instead, it was asserted that "Applicant's arguments have been previously presented (e.g. Remarks, 12/1/2009, 7/27/2009) and the Examiner notes that they are unpersuasive."

Appellant submits that the Final Office Action and the Advisory Action have ignored important features that appear in claim 1. Those features are:

     1)    "first data processor means"

     2)    "second data processor means"

     3)    "authenticate each other by a second authentication, responsive to the first authentication between the first processor means and the second data processor means"

For a reference to be properly used against Appellant's claim 1, the reference would need to show first and second data processor means which authenticate each other by a second authentication using second data, responsive to a first authentication. As will be described further below, although Tsuji teaches a microprocessor, Tsuji lacks first and second processor means that authenticate each other by a second authentication, responsive to a first authentication.

Appellant will next describe different remote control systems of Tsuji. Tsuji discloses, in Fig. 1, a remote control system including transmitter 1 and receiver 2. Transmitter 1 includes microprocessor 11 which enciphers a rolling code and uses the enciphered rolling code to produce a transmission code. (Paragraphs [0037-0041] and [0053]). Receiver 2 receives the transmission code from transmitter 1 and deciphers the enciphered rolling code [0042-0044].

Tsuji also discloses, in Fig. 10, an electronic key system including portable unit 30, vehicle transmitter 33 and wireless receiver 34. Portable unit 30 includes a transmitting/receiving circuit for receiving a challenge code signal (from transmitter 33) and transmitting an enciphered challenge code signal (to wireless

receiver 34).  Portable unit 30 includes a RAM for storing an ID code of portable unit and an enciphering table (Fig. 11).  (Paragraphs [0083-0085]).

At Figs. 17 and 18, Tsuji discloses a key code registration between portable unit 30 and vehicle 32.  As shown in Fig. 17, portable unit 30 produces and transmits a transmission code including an ID code and an enciphered key code to vehicle 32.  (Paragraphs [0109-0117]).  As shown in Fig. 18, vehicle 32 receives the transmission code from portable unit 30, extracts the ID code and restores the enciphered key code.  Vehicle 32 also compares the extracted ID code with a stored ID code of security ECU 35 to determine whether to store the restored key code.  (Paragraphs [0118-0121]).

Thus, Fig. 1 and paragraphs [0043-0044], [0049] and [0053] of Tsuji relate to a remote control system that teaches use of a rolling code to allow normal operation.  Separate and distinct from Fig. 1, Fig. 10 and paragraphs [0084], [0088] and [0090] of Tsuji relate to a remote control system that uses a challenge code to unlock a door.

Tsuji, however, does not disclose or suggest that first and second data processor means authenticate each other by:  1) a first authentication which includes passing and comparing first data between an immobilizer unit and a portable unit and 2) a second authentication responsive to the first authentication, which includes passing second data between the immobilizer unit and the portable unit, as required by claim 1 (emphasis added).  Tsuji et al. do not teach a second authentication using second data, responsive to the first authentication.  No identification of any such teaching in Tsuji has been provided.

Pages 8-9 of the Final Office Action merely relies on remote control systems shown in Figs. 1 and 10 of Tsuji to teach first and second authentication.  Appellant notes that Figs. 1 and 10 are different remote control systems.  In Tsuji, the rolling code (Fig. 1) is **not used responsive to** the challenge code (Fig. 10) (or vice versa).  Instead, the rolling code is used separately (in a different remote control system) from the challenge code.  Tsuji only teaches using one authentication, either a rolling code (Fig. 1) or a challenge code (Fig. 10).

In summary, Tsuji does not disclose or suggest Appellant's claimed features of first and second data processor means which authenticate each other using a first authentication (with first data) and a second authentication (with second data), responsive to the first authentication, as required by claim 1. As set forth above, these features are completely absent from Tsuji.

Appellant will now address another issue under appeal with respect to independent claim 1. Appellant submits that the Final Office Action and the Advisory Action have ignored additional limitations that appear in claim 1. Those limitations are:

1)      a portable unit including a "fourth storage ... preliminarily storing second data for mutual authentication different from the first data for mutual authentication"

2)      that the second authentication includes: "1) the second data processor means transmitting the second data for mutual authentication stored in the fourth storage..., 2) the first data processor means further storing, into the second storage, the second data for mutual authentication received via the first antenna and transmitting the second data for mutual authentication stored in the second storage..., and 3) the second data processor means further storing, into the third storage, the second data for mutual authentication received"

For a reference to be properly used against Appellant's claim 1, the reference would need to show passing second data for mutual authentication between the immobilizer unit and the portable unit by: 1) the portable unit passing preliminary second data stored in its fourth storage to the immobilizer unit, 2) the immobilizer unit storing the received second data in its second storage, 3) the immobilizer unit transmitting the second data that is in its second storage to the portable unit and 4) the portable unit storing the received second data in its third storage.

As discussed above, Tsuji does not teach mutual authentication by using second data. Accordingly, Tsuji cannot teach that:  a) the portable unit

includes a fourth storage for storing preliminary second data for mutual authentication, b) the second data is passed between the portable unit and the immobilizer unit based on the preliminary second data stored in the fourth storage of the portable unit and c) the portable unit subsequently stores second data (that has been received and stored by the immobilizer unit) into a third storage (i.e., a different storage from the preliminary stored second data), as recited by claim 1. Tsuji is silent regarding these indicated features. Thus, Tsuji does not include all of the features of claim 1.

Moreover, it is submitted that Hisada does not make up for the deficiencies of Tsuji with respect to claim 1. Hisada discloses, in Fig. 1, a vehicle security system including vehicle control unit 30 and remote-control unit 11. Vehicle control unit 30 produces a cryptographic code and remote-control unit 11 produces a cipher system code in response to the cryptographic code. (Col. 7, line 47 - Col. 8, line 5 and Col. 16, lines 48-55).

Hisada, however, does not disclose or suggest a mutual authentication process between first and second data processor means including 1) first authentication by passing and comparing first data between the immobilizer unit and the portable unit and 2) second authentication, responsive to the first authentication, by passing second data between the immobilizer unit and the portable unit, as required by claim 1. In addition, Hisada does not disclose or suggest passing the second data between the portable unit and the immobilizer unit based on preliminary second data stored in a fourth storage of the portable unit such that the portable unit also stores subsequently received second data in a third storage (from second data that has been stored by the immobilizer unit), as required by claim 1. Thus, Hisada cannot provide the features of claim 1 which are missing from Tsuji. Accordingly, allowance of claim 1 is respectfully requested.

Dependent claims 5-9 are patentable by virtue of their dependency on allowable independent claim 1.

E. **Rejection of Claim 2 under 35 U.S.C. § 103(a) as being unpatentable over Tsuji in view of Hisada.**

The aforementioned rejection is respectfully traversed for at least the reasons set forth below.

Appellant's claim 2 relates to a vehicle anti-theft system including an immobilizer unit and a portable unit. Particularly, independent claim 2, recites the following:

> ...an immobilizer unit including ... first data processor means ...; and a second storage... preliminarily storing second data for mutual authentication different from the first data for mutual authentication...

> ...a portable unit including... second data processor means...

> ...the first data processor means and the second data processor means authenticate each other by a first authentication comprising: (1) the first data processor means transmitting... an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data..., decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage; and

> ...the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the first data processor means transmitting the second data for mutual authentication that is stored in the second storage... and 2) the second data processor means storing, into the third storage, the second data for mutual authentication received... (Emphasis Added)

Appellant's claim 2 includes features which are neither disclosed nor suggested by the cited art. Namely, first and second data processor means, of the respective immobilizer unit and the portable unit, which authenticate each other by the combination of: 1) a first authentication which includes passing and comparing first data between the immobilizer and portable units and 2) a second authentication, responsive to the first authentication, which includes passing second data between the immobilizer and portable units. One issue under appeal is whether or not Tsuji or Hisada disclose or suggest first and second data processor means which authenticate each other by a second authentication using second data, responsive to the first authentication.

As discussed above with respect to independent claim 1, Tsuji does not disclose or suggest that first and second data processor means authenticate each other by: 1) a first authentication which includes passing and comparing first data between an immobilizer unit and a portable unit and 2) a second authentication responsive to the first authentication, which includes passing second data between the immobilizer unit and the portable unit, as required by claim 2 (emphasis added). Tsuji et al. do not teach a second authentication using second data, responsive to the first authentication. As discussed above, Tsuji teaches, in Figs. 1 and 10, different remote control systems, where each system uses one authentication, either a rolling code (Fig. 1) or a challenge code (Fig. 10). As set forth above with respect to claim 1, these features are completely absent from Tsuji.

Appellant will now address another issue under appeal with respect to independent claim 2. Appellant submits that the Final Office Action and the Advisory Action have ignored additional features that appear in claim 2. Those features are:

1)      an immobilizer unit including a "second storage... preliminarily storing second data for mutual authentication different from the first data for mutual authentication"

2)      that the second authentication includes:  "1) the first data processor means transmitting the second data for mutual authentication that is stored in the second storage via the first antenna and 2) the second data processor means storing, into the third storage, the second data for mutual authentication received via the second antenna"

For a reference to be properly used against Appellant's claim 2, the reference would need to show passing second data for mutual authentication between the immobilizer unit and the portable unit by: 1) the immobilizer unit passing preliminary second data stored in its second storage to the portable unit and 2) the portable unit storing the received second data in its third storage.

As discussed above, Tsuji does not teach mutual authentication by using second data. Accordingly, Tsuji cannot teach that: a) the immobilizer unit includes a second storage for storing preliminary second data for mutual

authentication, b) the second data is passed from the immobilizer unit to the portable unit based on the preliminary second data stored in the second storage of the immobilizer unit and c) the portable unit subsequently stores the received second data into its third storage, as recited by claim 2. Tsuji is silent regarding these indicated features. Thus, Tsuji does not include all of the features of claim 2.

Moreover, it is submitted that Hisada does not make up for the deficiencies of Tsuji with respect to claim 2. Hisada is discussed above. Hisada does not disclose or suggest a mutual authentication process between first and second data processor means including 1) first authentication by passing and comparing first data between the immobilizer unit and the portable unit and 2) second authentication, responsive to the first authentication, by passing second data between the immobilizer unit and the portable unit, as required by claim 2. In addition, Hisada does not disclose or suggest passing the second data between the immobilizer unit and the portable unit based on preliminary second data stored in a second storage of the immobilizer unit, as required by claim 2. Thus, Hisada cannot provide the features of claim 2 which are missing from Tsuji. Accordingly, allowance of claim 2 is respectfully requested.

Dependent claims 10-14 are patentable by virtue of their dependency on allowable independent claim 2.

**F. Rejection of Claim 3 under 35 U.S.C. § 103(a) as being unpatentable over Tsuji in view of Hisada.**

The aforementioned rejection is respectfully traversed for at least the reasons set forth below.

Appellant's claim 3 relates to a vehicle anti-theft system including an immobilizer unit and a portable unit. Particularly, independent claim 3, recites the following:

...an immobilizer unit including ... first data processor means ...

...a portable unit including... second data processor means...

...the first data processor means and the second data processor means authenticate each other by a first authentication

comprising: (1) the first data processor means transmitting... an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data..., decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage...

...the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the first data processor means requesting the second data processor means... to generate second data for mutual authentication different from the first data for mutual , 2) responsive to the request from the first data processor means, the second data processor means further generating, storing into the third storage, and transmitting..., the second data for mutual authentication, 3) the first data processor means storing, into the second storage, the second data for mutual authentication received... and transmitting the second data for mutual authentication stored in the second storage... and 4) the second data processor means further storing, into the third storage, the second data for mutual authentication received... (Emphasis Added)

Appellant's claim 3 includes features which are neither disclosed nor suggested by the cited art. Namely, first and second data processor means, of the respective immobilizer unit and the portable unit, which authenticate each other by the combination of: 1) a first authentication which includes passing and comparing first data between the immobilizer and portable units and 2) a second authentication, responsive to the first authentication, which includes passing second data between the immobilizer and portable units. One issue under appeal is whether or not Tsuji or Hisada disclose or suggest first and second data processor means which authenticate each other by a second authentication using second data, responsive to the first authentication.

As discussed above with respect to independent claim 1, Tsuji does not disclose or suggest that first and second data processor means authenticate each other by: 1) a first authentication which includes passing and comparing first data between an immobilizer unit and a portable unit and 2) a second authentication responsive to the first authentication, which includes passing second data between the immobilizer unit and the portable unit, as required by claim 3 (emphasis added).

Tsuji et al. do not teach a second authentication using second data, responsive to the first authentication. As discussed above, Tsuji teaches, in Figs. 1 and 10, different remote control systems, where each system uses one authentication, either a rolling code (Fig. 1) or a challenge code (Fig. 10). As set forth above with respect to claim 1, these features are completely absent from Tsuji.

Appellant will now address another issue under appeal with respect to independent claim 3. Appellant submits that the Final Office Action and the Advisory Action have ignored additional features that appear in claim 3. Those features are:

- that the second authentication includes: "1) the first data processor means requesting the second data processor means... to generate second data for mutual authentication different from the first data for mutual authentication, 2) responsive to the request from the first data processor means, the second data processor means further generating, storing into the third storage, and transmitting..., the second data for mutual authentication, 3) the first data processor means storing, into the second storage, the second data for mutual authentication received... and transmitting the second data for mutual authentication stored in the second storage... and 4) the second data processor means further storing, into the third storage, the second data for mutual authentication received..."

For a reference to be properly used against Appellant's claim 3, the reference would need to show passing second data for mutual authentication between the immobilizer unit and the portable unit by: 1) the immobilizer unit requesting the portable unit to generate the second data, 2) the portable unit generating, storing and transmitting the generated second data responsive to the request, 3) the immobilizer unit storing the received second data, 4) the immobilizer unit transmitting the stored second data and 5) the portable unit storing the subsequent received second data (from the immobilizer unit).

As discussed above, Tsuji does not teach mutual authentication by using second data. Accordingly, Tsuji cannot teach that: a) the portable unit generates second data responsive to a request from the immobilizer unit, b) the

second data is passed between the portable unit and the immobilizer unit based on second data generated by the portable unit and c) the portable unit subsequently stores received second data (that has been stored by the immobilizer unit), as recited by claim 3. Tsuji is silent regarding these indicated features. Thus, Tsuji does not include all of the features of claim 3.

Moreover, it is submitted that Hisada does not make up for the deficiencies of Tsuji with respect to claim 3. Hisada is discussed above. Hisada does not disclose or suggest a mutual authentication process between first and second data processor means including 1) first authentication by passing and comparing first data between the immobilizer unit and the portable unit and 2) second authentication, responsive to the first authentication, by passing second data between the immobilizer unit and the portable unit, as required by claim 3. In addition, Hisada does not disclose or suggest passing the second data between the portable unit and the immobilizer unit based on second data generated by the portable unit, such that the portable unit stores subsequent second data (stored by the immobilizer unit), as required by claim 3. Thus, Hisada cannot provide the features of claim 3 which are missing from Tsuji. Accordingly, allowance of claim 3 is respectfully requested.

Dependent claims 15-19 are patentable by virtue of their dependency on allowable independent claim 3.

**G. Rejection of Claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Tsuji in view of Hisada.**

The aforementioned rejection is respectfully traversed for at least the reasons set forth below.

Appellant's claim 4 relates to a vehicle anti-theft system including an immobilizer unit and a portable unit. Particularly, independent claim 4, recites the following:

...an immobilizer unit including ... first data processor means ...

...a portable unit including... second data processor means...

...the first data processor means and the second data processor means <u>authenticate each other by a first authentication</u> comprising: (1) the first data processor means transmitting... an encrypted data <u>based on the first data for mutual authentication</u> stored in the first storage and (2) the second data processor means receiving the encrypted data..., decrypting the encrypted data and <u>comparing the decrypted data to the first data for mutual authentication</u> stored in the third storage...

...the first data processor means and the second data processor means <u>authenticate each other by a second authentication, responsive to the first authentication</u> between the first data processor means and the second data processor means, comprising:  1) the first data processor means <u>generating</u>, storing into the second storage, and transmitting..., <u>second data for mutual authentication</u> different from the first data for mutual authentication and 2) the second data processor means <u>storing</u>, into the third storage, <u>the second data for mutual authentication</u> received... (Emphasis Added)

Appellant's claim 4 includes features which are neither disclosed nor suggested by the cited art. Namely, first and second data processor means, of the respective immobilizer unit and the portable unit, which authenticate each other by the combination of:  1) <u>a first authentication</u> which includes passing and comparing <u>first data</u> between the immobilizer and portable units and 2) <u>a second authentication, responsive to the first authentication</u>, which includes passing <u>second data</u> between the immobilizer and portable units.  One issue under appeal is whether or not Tsuji or Hisada disclose or suggest first and second data processor means which authenticate each other by a second authentication using second data, responsive to the first authentication.

As discussed above with respect to independent claim 1, Tsuji does not disclose or suggest that first and second data processor means authenticate each other by:  1) <u>a first authentication</u> which includes passing and comparing <u>first data</u> between an immobilizer unit and a portable unit <u>and</u> 2) <u>a second authentication responsive to the first authentication</u>, which includes passing <u>second data</u> between the immobilizer unit and the portable unit, as required by claim 4 (emphasis added). Tsuji et al. do not teach a <u>second authentication using second data, responsive to the first authentication</u>.  As discussed above, Tsuji teaches, in Figs. 1 and 10, different remote control systems, where each system uses <u>one authentication</u>, either a rolling

code (Fig. 1) or a challenge code (Fig. 10). As set forth above with respect to claim 1, these features are completely absent from Tsuji.

Appellant will now address another issue under appeal with respect to independent claim 4. Appellant submits that the Final Office Action and the Advisory Action have ignored additional features that appear in claim 4. Those features are:

- that the second authentication includes: "1) the first data processor means generating, storing into the second storage, and transmitting via the first antenna, second data for mutual authentication different from the first data for mutual authentication and 2) the second data processor means storing, into the third storage, the second data for mutual authentication received via the second antenna"

For a reference to be properly used against Appellant's claim 4, the reference would need to show passing second data for mutual authentication between the immobilizer unit and the portable unit by: 1) the immobilizer unit generating second data, storing the generated second data and transmitting the generated second data to the portable unit and 2) the portable unit storing the received second data.

As discussed above, Tsuji does not teach mutual authentication by using second data. Accordingly, Tsuji cannot teach that: a) the immobilizer unit generates second data for mutual authentication, b) the generated second data is passed from the immobilizer unit to the portable unit and c) the portable unit subsequently stores the received second data, as recited by claim 4. Tsuji is silent regarding these indicated features. Thus, Tsuji does not include all of the features of claim 4.

Moreover, it is submitted that Hisada does not make up for the deficiencies of Tsuji with respect to claim 4. Hisada is discussed above. Hisada does not disclose or suggest a mutual authentication process between first and second data processor means including 1) first authentication by passing and comparing first data between the immobilizer unit and the portable unit and 2) second authentication, responsive to the first authentication, by passing second data between the immobilizer unit and the portable unit, as required by claim 4. In
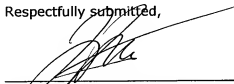
addition, Hisada does not disclose or suggest passing the second data from the immobilizer unit to the portable unit based on second data generated by the immobilizer unit, as required by claim 4. Thus, Hisada cannot provide the features of claim 4 which are missing from Tsuji. Accordingly, allowance of claim 4 is respectfully requested.

Dependent claims 20-24 are patentable by virtue of their dependency on allowable independent claim 4.

## **Conclusion**

Allowance of the identified application is respectfully requested.

Respectfully submitted,

Jacques L. Etkowicz, Reg. No. 41,738
Attorneys for Applicant

DMG/sh

Attachments:  Claims Appendix
              Evidence Appendix
              Related Proceedings Appendix

Dated:  August 12, 2010

P.O. Box 980
Valley Forge, PA  19482-0980
(610) 407-0700

1006600

# VIII. CLAIMS APPENDIX

1.    (Previously Presented)  A vehicle antitheft system comprising:

an immobilizer unit including:

first data processor means;

a first communication part connected with the first data processor means;

a first antenna connected with the first communication part;

a first storage connected with the first data processor means, the first storage preliminarily storing first data for mutual authentication; and

a second storage connected with the first data processor means; and

a portable unit including:

second data processor means;

a second communication part connected with the second data processor means;

a second antenna connected with the second communication part;

a third storage connected with the second data processor means, the third storage preliminarily storing the first data for mutual authentication; and

a fourth storage connected with the second data processor means, the fourth storage preliminarily storing second data for mutual authentication different from the first data for mutual authentication;

wherein:

the immobilizer unit further includes an information reception part connected with the first data processor means, and when a first instruction is fed into the information reception part, the first data processor means and the second data

processor means authenticate each other by a first authentication comprising: (1) the first data processor means transmitting via the first antenna an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data via the second antenna, decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage; and

the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the second data processor means transmitting the second data for mutual authentication stored in the fourth storage via the second antenna, 2) the first data processor means further storing, into the second storage, the second data for mutual authentication received via the first antenna and transmitting the second data for mutual authentication stored in the second storage via the first antenna, and 3) the second data processor means further storing, into the third storage, the second data for mutual authentication received via the second antenna.

2.    (Previously Presented)  A vehicle antitheft system comprising:

an immobilizer unit including:

first data processor means;

a first communication part connected with the first data processor means;

a first antenna connected with the first communication part;

a first storage connected with the first data processor means, the first storage preliminarily storing first data for mutual authentication; and

a second storage connected with the first data processor means, the second storage preliminarily storing second data for mutual authentication different from the first data for mutual authentication; and

a portable unit including:

second data processor means;

a second communication part connected with the second data processor means;

a second antenna connected with the second communication part; and

a third storage connected with the second data processor means, the third storage preliminarily storing the first data for mutual authentication;

wherein:

the immobilizer unit further includes an information reception part connected with the first data processor means, and when a first instruction is fed into the information reception part, the first data processor means and the second data processor means authenticate each other by a first authentication comprising: (1) the first data processor means transmitting via the first antenna an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data via the second antenna, decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage; and

the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the first data processor means transmitting the second data for mutual authentication that is stored in the second storage via the first antenna and 2) the second data processor means storing, into the third storage, the second data for mutual authentication received via the second antenna.

3.      (Previously Presented)  A vehicle antitheft system comprising:

an immobilizer unit including:

first data processor means;

a first communication part connected with the first data processor means;

a first antenna connected with the first communication part;

a first storage connected with the first data processor means, the first storage preliminarily storing first data for mutual authentication; and

a second storage connected with the first data processor means; and

a portable unit including:

second data processor means;

a second communication part connected with the second data processor means;

a second antenna connected with the second communication part; and

a third storage connected with the second data processor means, the third storage preliminarily storing the first data for mutual authentication;

wherein:

the immobilizer unit further includes an information reception part connected with the first data processor means, and when a first instruction is fed into the information reception part, the first data processor means and the second data processor means authenticate each other by a first authentication comprising: (1) the first data processor means transmitting via the first antenna an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data via the second antenna, decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage;

the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the first data processor means requesting the second data

processor means via the first antenna to generate second data for mutual authentication different from the first data for mutual , 2) responsive to the request from the first data processor means, the second data processor means further generating, storing into the third storage, and transmitting via the second antenna, the second data for mutual authentication, 3) the first data processor means storing, into the second storage, the second data for mutual authentication received via the first antenna and transmitting the second data for mutual authentication stored in the second storage via the first antenna and 4) the second data processor means further storing, into the third storage, the second data for mutual authentication received via the second antenna.

4.      (Previously Presented)  A vehicle antitheft system comprising:

an immobilizer unit including:

first data processor means;

a first communication part connected with the first data processor means;

a first antenna connected with the first communication part;

a first storage connected with the first data processor means, the first storage preliminarily storing first data for mutual authentication; and

a second storage connected with the first data processor means; and

a portable unit including:

second data processor means;

a second communication part connected with the second data processor means;

a second antenna connected with the second communication part; and

a third storage connected with the second data processor means, the third storage preliminarily storing the first data for mutual authentication;

wherein:

the immobilizer unit further includes an information reception part connected with the first data processor means, and when a first instruction is fed into the information reception part, the first data processor means and the second data processor means authenticate each other by a first authentication comprising: (1) the first data processor means transmitting via the first antenna an encrypted data based on the first data for mutual authentication stored in the first storage and (2) the second data processor means receiving the encrypted data via the second antenna, decrypting the encrypted data and comparing the decrypted data to the first data for mutual authentication stored in the third storage;

the first data processor means and the second data processor means authenticate each other by a second authentication, responsive to the first authentication between the first data processor means and the second data processor means, comprising: 1) the first data processor means generating, storing into the second storage, and transmitting via the first antenna, second data for mutual authentication different from the first data for mutual authentication and 2) the second data processor means storing, into the third storage, the second data for mutual authentication received via the second antenna.

5. (Previously Presented) The vehicle antitheft system according to claim 1, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, either the first data processor means generates and stores into the second storage first accumulation data different from the second data for mutual authentication, or the second data processor means generates and stores into the third storage the first accumulation data; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

6.    (Previously Presented)  The vehicle antitheft system according to claim 1, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, the first data processor means transmits the first data for mutual authentication stored in the first storage via the first antenna, and the second data processor means stores, into the third storage, the first data for mutual authentication received via the second antenna; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

7.    (Previously Presented)  The vehicle antitheft system according to claim 1, wherein the portable unit further has a fifth storage preliminarily storing an ID code, and the first data processor means and the second data processor means authenticate each other also using the ID code.

8.    (Previously Presented)  The vehicle antitheft system according to claim 7, wherein the immobilizer unit further has a sixth storage, the second data processor means transmits, via the second antenna, the ID code stored in the fifth storage, and the first data processor means stores, into the sixth storage, the ID code received via the first antenna.

9.    (Previously Presented)  The vehicle antitheft system according to claim 8, wherein upon input of a second instruction into the information reception part, the first data processor means generates third accumulation data different from the ID code stored in the sixth storage, and stores the third accumulation data into the sixth storage.

10.    (Previously Presented)  The vehicle antitheft system according to claim 2, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, either the first data processor means generates and

stores into the second storage first accumulation data different from the second data for mutual authentication, or the second data processor means generates and stores into the third storage the first accumulation data; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

11.     (Previously Presented) The vehicle antitheft system according to claim 2, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, the first data processor means transmits the first data for mutual authentication stored in the first storage via the first antenna, and the second data processor means stores, into the third storage, the first data for mutual authentication received via the second antenna; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

12.     (Previously Presented) The vehicle antitheft system according to claim 2, wherein the portable unit further has a fifth storage preliminarily storing an ID code, and the first data processor means and the second data processor means authenticate each other also using the ID code.

13.     (Previously Presented) The vehicle antitheft system according to claim 12, wherein the immobilizer unit further has a sixth storage, the second data processor means transmits, via the second antenna, the ID code stored in the fifth storage, and the first data processor means stores, into the sixth storage, the ID code received via the first antenna.

14.    (Previously Presented)  The vehicle antitheft system according to claim 13, wherein upon input of a second instruction into the information reception part, the first data processor means generates third accumulation data different from the ID code stored in the sixth storage, and stores the third accumulation data into the sixth storage.

15.    (Previously Presented)  The vehicle antitheft system according to claim 3, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, either the first data processor means generates and stores into the second storage first accumulation data different from the second data for mutual authentication, or the second data processor means generates and stores into the third storage the first accumulation data; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

16.    (Previously Presented)  The vehicle antitheft system according to claim 3, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, the first data processor means transmits the first data for mutual authentication stored in the first storage via the first antenna, and the second data processor means stores, into the third storage, the first data for mutual authentication received via the second antenna; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

17.    (Previously Presented)  The vehicle antitheft system according to claim 3, wherein the portable unit further has a fifth storage preliminarily storing an ID code, and the first data processor means and the second data processor means authenticate each other also using the ID code.

18.    (Previously Presented)  The vehicle antitheft system according to claim 17, wherein the immobilizer unit further has a sixth storage, the second data processor means transmits, via the second antenna, the ID code stored in the fifth storage, and the first data processor means stores, into the sixth storage, the ID code received via the first antenna.

19.    (Previously Presented)  The vehicle antitheft system according to claim 18, wherein upon input of a second instruction into the information reception part, the first data processor means generates third accumulation data different from the ID code stored in the sixth storage, and stores the third accumulation data into the sixth storage.

20.    (Previously Presented)  The vehicle antitheft system according to claim 4, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, either the first data processor means generates and stores into the second storage first accumulation data different from the second data for mutual authentication, or the second data processor means generates and stores into the third storage the first accumulation data; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

21.    (Previously Presented)  The vehicle antitheft system according to claim 4, wherein, upon input of a second instruction into the information reception part, when both of data stored in the second storage and the third storage are the second data for mutual authentication, the first data processor means transmits the first

data for mutual authentication stored in the first storage via the first antenna, and the second data processor means stores, into the third storage, the first data for mutual authentication received via the second antenna; and

when both of data stored in the second storage and the third storage are identical to the first data for mutual authentication, either the first data processor means generates and stores into the second storage second accumulation data different from the first data for mutual authentication, or the second data processor means generates and stores into the third storage second accumulation data different from the first data for mutual authentication.

22. (Previously Presented) The vehicle antitheft system according to claim 4, wherein the portable unit further has a fifth storage preliminarily storing an ID code, and the first data processor means and the second data processor means authenticate each other also using the ID code.

23. (Previously Presented) The vehicle antitheft system according to claim 22, wherein the immobilizer unit further has a sixth storage, the second data processor means transmits, via the second antenna, the ID code stored in the fifth storage, and the first data processor means stores, into the sixth storage, the ID code received via the first antenna.

24. (Previously Presented) The vehicle antitheft system according to claim 23, wherein upon input of a second instruction into the information reception part, the first data processor means generates third accumulation data different from the ID code stored in the sixth storage, and stores the third accumulation data into the sixth storage.

## IX.  <u>EVIDENCE APPENDIX</u>

None

## X. **RELATED PROCEEDINGS APPENDIX**

None